UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,004	12/21/2001	Robert R. Gilman	013217.0177PTUS	2388

24283 7590 06/26/2008

PATTON BOGGS LLP
1801 CALFORNIA STREET
SUITE 4900
DENVER, CO 80202

EXAMINER	
BROWN, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ROBERT R. GILMAN, RICHARD L. ROBINSON and
DOUGLAS A. SPENCER

Appeal 2007-1049
Application 10/028,004[1]
Technology Center 2100

Decided: June 26, 2008

Before RICHARD E. SCHAFER, JAMESON LEE and SALLY C. MEDLEY, *Administrative Patent Judges*.

MEDLEY, *Administrative Patent Judge*.

DECISION ON APPEAL

[1] Application for patent filed 21 Dec. 2001.
The real party in interest is Avaya Technology Corp.

A. Statement of the Case

This is an appeal under 35 U.S.C. § 134 from the Examiner's Final Rejection of claims 1-15 and 18[2]. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Chang et al.	5,724,425	Mar. 03, 1998
Horstmann	6,044,469	Mar. 28, 2000
Ho et al.	2002/0073325	Jun. 13, 2002

Claims 1-5 and 10-14 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Chang et al. ("Chang") and Ho et al. ("Ho").

Claims 6-9, 15 and 18 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Chang, Ho and Horstmann.

BACKGROUND

The invention is related to a secure data authentication apparatus. The secure data authentication apparatus authenticates the source of a software file for use on a computer system having a secure processing device. The secure data authentication apparatus authenticates an owner of the software file. The secure data authentication apparatus also authenticates that the owner of the software file is the owner of the computer system on which the software file is being installed. The software file includes a first source signature and a unique owner signature. The secure processing device generates a second source signature and a second owner signature. If the first and second source signatures match and the first and second owner signatures match, the computer system accepts the software file as

[2] Claims 16-17 were cancelled by the Applicants in the Amendment filed 06 Feb. 2006.

authenticated for the owners use and from the source represented by the first source signature. (Abs. and Spec. 6-7)

B. Issues

The issues are (1) whether the Applicants have shown that the Examiner erred in determining claims 1-5 and 10-14 are unpatentable under 35 U.S.C. § 103(a) over Chang and Ho and (2) whether the Applicants have shown that the Examiner erred in determining claims 6-9, 15 and 18 are unpatentable under 35 U.S.C. § 103(a) over Chang, Ho and Horstmann?

For the reasons that follow, the Applicants have failed to show that the Examiner erred in determining (1) that claims 1-5 and 10-14 are unpatentable over Chang and Ho and (2) that claims 6-9, 15 and 18 are unpatentable over Chang, Ho and Horstmann.

C. Findings of Facts ("FF")

The record supports the following findings of facts as well as any other findings of fact set forth in this opinion by at least a preponderance of the evidence.

1.Applicants' claims 1-15 and 18 are the subject of this appeal.

2.Claims 1, 7, 10, 11 and 18 are independent.

3.Claims 2-6, 8-9 and 12-15 are directly or indirectly dependent on claims 1, 7 and 11 respectively.

4.Claims 1-15 and 18 stand or fall together since the Applicants did not argue the claims separately (App. Br. 12, 14).

5.Applicants indicate that claim 1 is representative of all the claims (App. Br. 14).

6.Claim 1 is as follows:

> A secure data authentication apparatus to authenticate a software file, the software file having a first signature appended to the software file, for use on a computer system, wherein said computer system is assigned an owner key that is unique to said computer system, said first signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature, the apparatus comprising:
>
> a secure processing device within the computer system to receive the software file and hash the software file using said selected hash function to produce a first hash value; and
>
> a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature and compares the first signature with the second signature, and if the first signature matches the second signature, the computer system accepts the software file as being authenticated.

7.The Examiner found that Chang describes hashing a file to produce a hash value because Chang describes a message digest and explains that any known message digest algorithm such as MD2, MD4 or MD5 can be used to create the message digest (Final Rejection 4, Ans. 4 and Chang col. 7, ll. 1-20).

8.The Examiner also found that Chang describes encrypting the hash value with a key to generate a signature (Final Rejection 4, Ans. 4 and Chang col. 7, ll. 1-5).

9.The Examiner further found that Chang describes comparing the generated signature with the original signature (Final Rejection 4-5, Ans. 4 and Chang col. 9, ll. 37-47, figs. 6a, 6b).

10.The Examiner found that Chang also describes that the software files are authenticated if the signatures match (Final Rejection 5, Ans. 4 and Chang col. 9, ll. 45-46).

11.The Examiner found that Chang does not describe the implementation of an owner key that is unique to a given computer system (Final Rejection 3 and Ans. 3).

12.The Examiner found that Ho describes the use of a key specific to the individual computer system (Final Rejection 3, Ans. 3 and 6, and Ho ¶33).

13.The Examiner found, based on Chang's disclosure, that one with ordinary skill in the art would recognize that it is desirable to maintain the authenticity of a software program from malicious attack by worms, viruses, and other programs or individuals that have the intent of harming a host system (Final Rejection 3, Ans. 3 and Chang col. 1, l. 50-col. 3, l. 13).

14.The Examiner found that Chang describes that attacks on a host system are avoidable by implementing a signature system composed of a message digest (Final Rejection 3-4, Ans. 3 and Chang col. 1, l. 50-col. 3, l. 13).

15.The Examiner also found that Ho describes that a greater level of security may be obtained by the implementation of a unique key signature of a system so as to prevent a particular license from being compromised (Final Rejection 4, Ans. 3 and Ho ¶¶ 4-12).

16.The Examiner concluded that it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine the system of Ho into that of Chang for the advantages described above (Final Rejection 4 and Ans. 3-4).

17.The Examiner explains that the combination of Chang and Ho systems includes the unique identifier of the Ho system implemented for the key system of Chang (Final Rejection 4 and Ans. 4).

18.The Examiner further explains that Chang's ability to protect the integrity of the software system is maintained in the software system modified by Ho to include uniquely defining the entitlement of the license to the specific computer system (Final Rejection 4 and Ans. 4).

19.Ho describes two different methods of restricted software entitlement. (Ho ¶¶ 5).

20.Ho describes a first common method which is to encode hardware specific information in the computer system (Ho ¶¶ 5).

21.The second method is to make the software unique for each computer system and uniquely compile the software for each distribution.

22.Ho characterizes the second method as very costly (Ho ¶¶ 5).

23.Ho also describes that the entire system software embedded in an Internet Appliance can be stored in a compact and portable storage medium making it easy to illegally duplicate (Ho ¶¶ 9).

24. Ho also describes that users may back up the protected software without restriction (i.e. make a back up copy on a portable storage medium) (Ho ¶ 16).

25.Ho is not directed to protecting Internet Appliances from unauthorized copying (Ho ¶¶ 10, 13, 16).

26.Ho is directed to controlling the use and execution of embedded software in a computer system and restricting copies of the software from use in unauthorized computer systems (Ho ¶¶ 10, 13, 16).

D. Principles of Law

> "Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references." *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986).

> In an obviousness analysis, it is not necessary to find precise teachings in the prior art directed to the specific subject matter claimed because

inferences and creative steps that a person of ordinary skill in the art would employ can be taken into account. *See KSR International Co. v. Teleflex Inc.,* 127 S.Ct. 1727, 1741 (2007).

In *In re Gurly*, 27 F. 3d 551, 443 (Fed. Cir 1994), the Federal Circuit stated:

> A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant.

It is not required that the prior art teaching relied upon disclose the same problem as faced by the applicant, because all that is required is that the prior art provide some motivation or suggestion to combine the references. *In re Dillon*, 919 F.2d 688 (Fed. Cir. 1990) (in banc), *cert. denied*, 111 S.Ct. 1682 (1991).

E. Analysis

Claims 1-15 and 18 stand or fall together (FF[3] 4). We focus our analysis on independent claim 1 (FF 5). The Examiner rejected claim 1 as unpatentable under 35 U.S.C. § 103(a) over Chang and Ho. The Examiner found that Chang describes the claimed limitations with the exception of implementing an owner key that is unique to the given computer system (FFs 7-11). The Examiner found that Ho describes the use of a key specific to the individual computer system (FF 12).

[3] FF denotes Finding of Fact.

The Examiner found, based on Chang's disclosure, that one with ordinary skill in the art would recognize that it is desirable to maintain the authenticity of a software program from malicious attack by worms, viruses, and other programs or individuals that have the intent of harming a host system (FF 13). The Examiner found that Chang describes that attacks on a host system are avoidable by implementing a signature system composed of a message digest (FF 14). The Examiner found that Ho describes that a greater level of security may be obtained by implementing a unique key signature to a system so as to prevent a particular license from being compromised (FF 15). The Examiner concluded that it would have been obvious to one with ordinary skill in the art at the time the invention was made to combine the system of Ho into that of Chang for these stated advantages (FF 16). The Examiner explains that the combination of the Chang and Ho systems would result in the unique identifier of the Ho system implemented for the key system of Chang (FF 17). The Examiner further explains that Chang's ability to protect the integrity of the system software is maintained when modified by Ho, resulting in uniquely defining the entitlement of the license to the specific computer system (FF 18).

The Applicants argue that the Examiner has failed to establish a prima facie showing of obviousness because the Examiner has failed to cite and apply references which describe all of the Applicants' claimed elements or limitations (App. Br. 8-9 and 13-14). The Applicants submit that Chang and Ho do not describe the following limitations of claim 1:

- "the software file having a first signature appended to the software file"
- "said computer system is assigned an owner key that is unique to said computer system,"

- "source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature," and
- "a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature" (App. Br. 15).

In support of their arguments, the Applicants provide a claim chart. The claim chart includes claim 1 with certain elements underlined. Next to the claim is a column with the heading "Chang Patent." Beside that column is anther entitled "Ho Published Patent Application." Below each of these respective columns is Applicants' summary of the Chang and Ho references purportedly explaining why each of the references fail to describe the underlined claim 1 elements (App. Br. 15).

The Applicants' claim chart analysis is not helpful to the trier of fact and certainly does not rise to the level of showing error in the Examiner's findings. The Applicants' claim chart amounts to an attack against the Chang and Ho references individually. For example, under the "Chang Patent column" the Applicants argue that Chang does not describe a unique owner's key assigned to a destination computer. The Examiner relied on Ho to meet the "owner key" limitation, not Chang. The Examiner's rejection is based on the combination of the references. Thus, the inquiry becomes: do the combined teachings of Chang and Ho render the claimed invention obvious, not whether each and every individual reference describes each and every claimed limitation. The Examiner's rejection is based on obviousness, not anticipation. Moreover, the Applicants' argument (under the "Ho Published Patent Application" column), that Ho does not describe a computer system assigned a unique owner's key is without explanation of why that is so. The Examiner found that Ho describes a unique owner's key, directing attention to paragraph 33 of Ho (FF12). That paragraph of Ho describes using a computer system's *MAC address* "to generate the computed encrypted signature for the user." The Applicants have not addressed in any meaningful way why Ho's description of a computer system's MAC address is not a unique "owner key."

The Applicants also assert that neither Chang nor Ho describe *assigning a unique owner's key to a destination computer* (App. Br. 15-16). The Applicants argue that because both Chang and Ho do not describe an owner's key that is assigned to a destination computer, the references therefore do not describe computing a first signature which includes a hash value encrypted by the owner's key nor encrypting the first hash value with the owner's key to generate a second signature (App. Br. 16).

First, we are unable to find any reference to a *destination computer* in the language of claim 1. We are uncertain what the Applicants have in mind when they use the term "destination computer."

Second, Applicants are once again attacking the Chang and Ho references individually instead of considering the combination of the references. As explained above, the Examiner found that Ho describes the use of a key specific to the individual computer system (FF 12). As explained by the Examiner, the combination of Chang and Ho would result in a unique identifier (i.e. the key specific to the individual computer system described in Ho) for the key system of Chang (FF 17). The Applicants have not shown error in the Examiner's findings or conclusion of law.

The Applicants also argue that the Examiner has not provided an indication in the cited references that would provide a motivation or suggestion for combining the teachings of Chang and Ho that would render the Applicants' invention obvious (App. Br. 12, 16). However, it is not necessary to find precise teachings in the prior art directed to the specific subject matter claimed because inferences and creative steps that a person of ordinary skill in the art would employ can be taken into account.

The Examiner concluded that it would have been obvious to one with ordinary skill in the art to combine the references in order to (1) maintain the authenticity of a software program from malicious attack by worms, viruses, and other programs or individuals and (2) prevent a particular license of the computer system software from being compromised (FFs 13-16). The Applicants have not persuasively demonstrated why (1) maintaining the authenticity of a software program from malicious attack by worms, viruses, and other programs or individuals or (2) preventing a particular license of the computer system software from being compromised is an improper or insufficient motivation for one with ordinary skill in the art to combine the references.

The Applicants also argue that Chang and Ho teach away from the claimed invention (App. Br. 12, 17). More specifically, the Applicants argue that Ho specifically rejects the combination claimed by the Applicants since Ho describes the use of a computer specific encoding as impractical (App. Br. 12). We find the Applicants' reading of the Ho reference to be misplaced because Ho actually describes two different methods of restricted software entitlement (FF 19). Ho describes a first common method which is to encode hardware specific information in the computer system (FF 20).

The second method is to make the software unique for each computer system and uniquely compile the software for each distribution (FF 21). It is the latter which Ho characterizes as very costly (FF 22). Thus, Ho explains that it is very costly to make software unique for each computer, but does not characterize encoding hardware specific information in a computer system as impractical. For these reasons, the Applicants' teaching away theory is misplaced.

The Applicants also argue that Ho is limited to a self-contained storage medium and a network interface card (App. Br. 10). The Applicants further argue that Ho does not envision transmission of programs over a network to an end user computer because Ho relies on the software to be distributed as part of the hardware of an Internet Appliance (App. Br. 11-12). We are unable to understand the significance of these arguments. Claim 1 does not require the transmission of programs over a network to an end user computer. We again find the Applicants' reading of the Ho reference to be misplaced. In addition to describing the system software embedded on a self contained storage medium, Ho also describes that the entire system software embedded in an Internet Appliance can be stored in a compact and portable storage medium making it easy to illegally duplicate (FF 23). Ho also describes that users may back up the protected software without restriction (i.e. make a back up copy on a portable storage medium) (FF 24). Thus, the system software could also be distributed via portable storage media. It is not necessarily limited to distribution only as part of the hardware of the Internet Appliance as asserted by the Applicants. Moreover, even if we assume that the use of computer specific encoding is impractical and the system software can only be distributed as part of the hardware, the

Applicants have not persuasively demonstrated that one with ordinary skill in the art would be discouraged from following the path set out in Ho, or would be led in a direction divergent from the Applicants' path.

The Applicants also argue that the existence of a prior art reference (i.e. Ho) that teaches an owner key is irrelevant if the reference fails to address the same problem that is addressed by the Applicants' claims or the teachings of Chang (Reply Br. 1). The Applicants assert that their claims are also directed to simultaneously ensuring that a program purchased to execute on a specific processor runs only on that processor (Reply Br. 2). Claim 1 does not require simultaneously ensuring that a program purchased to execute on a specific processor runs only on that processor. The Applicants' arguments are not commensurate in scope with the language of the claim. Furthermore, there is no requirement that the prior art teaching relied upon disclose the same problem as faced by the Applicants.

Last, the Applicants also argue that Chang and Ho, on a global level, are both directed to computer software security systems, which is insufficient to support a motivation to combine the teachings of these two references (Reply Br. 2). Applicants further argue that Chang and Ho address different security concerns; guaranteeing the authenticity of the software program and protecting Internet Appliances from unauthorized copying (Reply Br. 2). We again find the Applicants characterization of the Ho reference to be misplaced. Ho is not directed to protecting *Internet Appliances* from unauthorized copying as asserted by the Applicants (FF 25). Instead, Ho is directed to controlling the use and execution of embedded software in a computer system and restricting copies of the software from being used in unauthorized computer systems (FF 26).

For all these reasons, we find that the Applicants have failed to show that the Examiner erred in determining that claim 1 is unpatentable over Chang and Ho. Since the Applicants indicated that claim 1 is representative of all the claims (FF 5) and all the claims stand or fall together (FF 4), we also find that the Applicants have failed to show that the Examiner erred in determining that claims 2-5 and 10-14 are unpatentable over Chang and Ho and claims 6-9, 15 and 18 are unpatentable over Chang, Ho and Horstmann.

Decision

Upon consideration of the record, and for the reasons given, the Examiner's rejections of claims 1-5 and 10-14 under 35 U.S.C. § 103(a) as unpatentable over Chang and Ho and claims 6-9, 15 and 18 under 35 U.S.C. § 103(a) as unpatentable over Chang, Ho and Horstmann are affirmed.

AFFIRMED

MAT

PATTON BOGGS LLP
1801 CALFORNIA STREET

SUITE 4900
DENVER CO 80202